

упатство

Преземање сертификат користејќи Mozilla Firefox ESR

Верзија: 5.1

Датум: 31.01.2022

103.11

КИБС АД Скопје

©2022 КИБС АД Скопје, сите права задржани

http://www.kibstrust.com/



Содржина

1.	Како да го преземам сертификатот?	2
2.	Како да проверам дека сертификатот е добро инсталиран?	5
3.	Како да направам безбедносна копија од сертификатот?	9
4.	Како да го импортирам сертификатот во Internet Explorer?	11
5.	Проверка на коренски сертификати во Internet Explorer	14

1. Како да го преземам сертификатот?

Од сертификати кои ги нуди КИБС ИС, сертификатите Verba Sign Adv, Verba Sign Pro Adv и Verba Seal Adv се генерираат на дискот на вашиот компјутер.

За да преземете еден од горенаведените сертификати, Ве молиме да го користете го веб прелистувачот Mozilla Firefox ESR, верзија која не е повисока од 68.3, која можете да ја преземете од веб локцијата: <u>https://ftp.mozilla.org/pub/firefox/releases/68.3.0esr/</u>, каде бирате подфолдер <u>win64/</u> за 64 или <u>win32/</u> за 32-битна верзија на Firefox.

Потоа, следете ги следните чекори:

- 1. Првин, отворете го веб прелистувачот Mozilla Firefox ESR, при што внимавајте да не направи Upgrade, па отворете го линкот <u>https://e-shop.kibstrust.com/raweb</u> во него.
- 2. На веб страната (Слика 1) внесете:
 - Нарачка: внесете го бројот на нарачка кој ви е испратен во истата електронска порака
 - E-mail: внесете ја e-mail адресата која ја наведовте во формуларот за барање за сертификат

и кликнете Потврди.

	ПРЕЗЕМАЊЕ DOWNLO	E HA CEPTIC AD CERTIFIC	ФИКАТ/ САТЕ	
Verba Sign	Аду Рг	о Аdv	erba Seal	Д аду Аду
99522236	insert information	n for your certifi	icate order	
mari rima 25 2021@o	mail.com			



 Ќе ви се отвори страната за потврда на податоците од регистрација (на Слика 2 е прикажан пример за Verba Sign Pro Adv сертификат). Проверете ги податоците и внесете Фраза за автентикација, без интерпункциски знаци. Изберете High Grade кај Јачина на енкрипција. Кликнете Submit (Потврди).

Symantec. Enrollment									
Help with this Page Потврда на податоците од порачката/ Confirm data from purchase order									
Податоци кои ги внесовте за Вашиот сертификат/Data for Your Certificate Податоците ги пополнивте при поднесувањето на порачката за сертификат. Полињата обележани со ѕвезда (*) ќе бидат содржани во Вашиот сертификат и ќе можат да бидат видени како детали на сертификатот. The data that were fulfilled during purchase order for certificate. Fields marked with an asterisk (*) are included with your Certificate and are viewable in the certificate's details.									
Име/First Nam	ie: *	Mari							
Презиме/Last	Name: *	Rima							
e-mail адреса лице/e-mail a person: *	на физичкото ddress of the natural	mari.rima.25.2021@gmail.co							
Назив на прав person name:	но лице/Legal *	PravnoLice							
Организацион Unit: *	ен дел/Organization	Oddel							
Работна позиц лице/Job posi person: *	ија на физичкото tion of natural	tester							
ЕДБ/VАТ: *		147852							
Нарачка број,	Order No:	99522236							
2.5.4.97= NTR-	EMEC/LEID: *	NTRLU-15823							
Регистрациски Number: *	i 6poj/Registration	6134							
Држава(на фі лице)/Country person): *	ізичкото /(of the natural	DK							

Фраза за автентикација/Challenge Phrase Фразата за автентикација е уникатна фраза која Ве заштитува од неавторизирани активности врз Вашиот сертификат. Не ја споделувајте. Внимавајте да не ја изгубите. Таа е потребна за поништување на Вашиот сертификат.

The Challenge Phrase is a unique phrase that protects you against unauthorized action on your Certificate. Do not share it with anyone. Do not lose it. You will need it when you want to revoke your Certificate.

Внесете фраза за автентикација/Enter Challenge Phrase: (задолжително)/(required) Не употребувајте интерпункциски знаци/Do not use any punctuation.

Опционално: Изберете јачина на ен Encryption Strength Ви препорачуваме да го оставите како што е this as it is.	ікрипција/ Optional: Choose Your предефинирано./ We recommend that you leave
	High Grade 🗸
Ако внесените информации се точ кликнете Поднеси за да продолж correct, click Submit to continue.	іни, кете/ If all the information above is Cancel
Copyright © 2014. Symantec Corporation. All rights reserved.	Symantec



4. По кликнување на копчето **Submit (Потврди)**, ќе ви се јави порака како на Слика 3. Уште еднаш проверете ја е-mail адресата и кликнете **ОК** ако сè е во ред.

Message	from webpage	×
?	Confirm your e-mail address: ime.prezime@domain.mk	
	If your e-mail address is correct, click OK. If not, click CANCEL and correct it in the enrollment form.	
	If the e-mail address is not correct, you will not be able to use your Digital ID.	
	OK Cancel	



5. По кликнување на **ОК** ќе се појави прозорче како на Слика 4, кое Ве информира дека во тек е генерирањето на парот клучеви за вашиот сертификат. Ве молиме почекајте.



Слика 4

6. Потоа започнува процесот на генерирање на Вашиот сертификат. Ве молиме почекајте додека трае овој процес (Слика 5).



Слика 5

7. Ќе ви се јави порака дека Вашиот сертификат е инсталиран (Слика 6). Кликнете ОК.



Слика 6

 Потоа, на веб страната ќе се прикаже дека сертификатот е генериран и инсталиран (Слика 7)!

'our Digital ID Inforn	ation.
\$ Country = MK Email Address = in \$ \$ Common Name = 1 Serial Number = 4	ie.prezime@domain.com me Prezime 02d93e4b6ca83861b7d68b2b37e7c6e
Consult our Help I	Neck and Tutorials:
 Go to the <u>Help</u> Go to the <u>Digi</u> services 	best one records. <u>Desk</u> to view our tutorials and other useful information. tal ID Center to find out more about Digital IDs and Digital ID

Слика 7

2. Како да проверам дека сертификатот е добро инсталиран?

По добивање на пораката дека Вашиот сертификат е успешно инсталиран, потребно е да проверите дали истиот е додаден во листата на персонални сертификати во веб прелистувачот. За да ја направите оваа проверка, извршете ги следните чекори:

1. Од менито на прелистувачот во горен десен агол селектирајте Options (Слика 8):

G Google	× ☆ Options	× +		- 🗆 ×
$\leftarrow \rightarrow$ C $\textcircled{0}$	https://www.google.com	80% 🛡 🟠	C Search	
			🕄 Sign in to Syn	ic
			Rew Window	Ctrl+N
			🗢 New Private V	Vindow Ctrl+Shift+P
			Restore Previo	ous Session
			Zoom	- 80% + 27
	Go	odle	Edit	ኤ 🖻 🔒
		gie	Library	>
			Add-ons	Ctrl+Shift+A
			🚃 🔅 Options	
			🖍 Customize	
	Пребарување на Goog	gle Ме следи среќа	Open File	Ctrl+ O
			Save Page As	Ctrl+S
	Google пон)	ди во: English	Print	
			Q Find in This P	age Ctrl+F
			More	>
			Web Develop	er >
			(?) Help	>
			🖒 Exit	Ctrl+Shift+Q

Слика 8

2. Во новиот прозорец (Слика 9) од менито на левата страна изберете ја опцијата **Privacy & Security,** отидете најдолу, притиснете на копчето **View Certificates**:

G Google	× 🔆 Options 🛛 ×	+		—		×			
$\overleftarrow{\leftarrow}$ \rightarrow C $\widehat{\mathbf{u}}$	Sirefox about:preferences#privacy	80% 🟠	Q Search		lii\ (D =			
		₽ Find in O	ptions			^			
🔆 General	Allow Firefox to send <u>c</u> rash reports to Mozilla	Learn more							
Q Search									
A Privacy & Security	Privacy & Security Security								
C Firefox Account	Deceptive Content and Dangerous Softwar								
	✓ <u>B</u> lock dangerous and deceptive content Lear								
	✓ Block <u>d</u> angerous downloads								
	✓ Warn you about unwanted and un <u>c</u> ommo								
	Certificates								
	When a server requests your personal certificate								
	Select one automatically								
	• <u>A</u> sk you every time								
	Query OCSP responder servers to confirm the	current validity of	View <u>C</u> ertificates						
③ Firefox Support	certificates		Security <u>D</u> evices						
						*			

Слика 9

3. Ако Вашиот сертификат е успешно инсталиран, тој ќе се наоѓа во листата на сертификати во картичката **Your Certificates** (Слика 10):

	Certificate Manager	
Your Certificates	People Servers Authorities	
/ou have certificates from	n these organizations that identify you	
Certificate Name	Security De Serial Nu Expires On	E
✓ KIBS AD Skopje		^
Imetest Pr Softwa	re Secu 23:6E:38:E4: Friday, August 26, 2022	
Test OneID	Software Secu 48:D5:0C:A9: Thursday, January 30, 2.	
ajde denes	Software Secu 33:02:D9:02: Sunday, December 8, 2.	
LILE JHKH	Software Secu 60:95:74:61: Saturday, September 1	
Imetest Prezime ze.	Software Secu 23:6E:38:E4: Friday, August 26, 2022	
TEST KIBS AD Skopj	e Software Secu 3A:72:15:C5: Saturday, August 6, 202	2
Lile STSkopje	Software Secu 10:E3:40:C2: Sunday, July 31, 2022	~
<u>V</u> iew <u>B</u> acku	p Backup All Import Delete	
	OF	<

Слика 10

Кликнете на <u>V</u>iew и ќе ви се прикаже нов прозорец во кој е даден преглед на подетални информации за истиот. Во картичката General (

Слика 11) дадени се општите информации за сертификатот:

Issued to: Податоци за субјектот за кој е издаден сертификатот и серискиот број на сертификатот

Issued by: Податоци за Издавачот на сертификати (KIBSTrust Issuing Qsig CA G2 или KIBSTrust Issuing Qseal CA G2)

Validity: Датум на издавање и датум на истекување на периодот на важење.

SSL Client Certificate	······································	
Email Signer Certificat	ie	
Issued To		
Common Name (CN)	Imetest Prezime zemiodelec	
Organization (O)	<not certificate="" of="" part=""></not>	
Organizational Unit (O	J) <not certificate="" of="" part=""></not>	
Serial Number	23:6E:38:E4:BF:9E:9F:3E:74:55:9C:EE:68:8A:4D:4C	
Issued By		
Common Name (CN)	KIBSTrust Issuing Qsig CA G2	
Organization (O)	KIBS AD Skopje	
Organizational Unit (O	U) KIBSTrust Services	
Period of Validity		
Begins On	Wednesday, August 25, 2021	
Expires On	Friday, August 26, 2022	
Fingerprints		
SHA-256 Fingerprint	33:9F:A9:F8:99:83:EE:2F:84:5A:DE:26:B5:65:C2:88: AB:EC:9B:8E:FA:D9:F3:8D:F7:17:37:FD:24:F7:D7:7C	
SHA1 Fingerprint	92:B6:9F:52:63:4B:CD:22:06:37:FB:C7:6F:C4:E2:34:F5:52:3B:9C	

Слика 11

Во картичката **Details** (Слика 12) се прикажуваат коренските сертификати (Certificate Hierarchy) со кои е потпишан Вашиот сертификат. Проверете дали се прикажуваат 2 коренски сертификати: **KIBSTrust Root CA G2** (Root сертификат) и **KIBSTrust Issuing Qsig CA G2** или **KIBSTrust Issuing QSealCA G2** како издавачки сертификати.

Certifica	te Viewer: "Imetest Prezime zemjodelec"	
<u>G</u> eneral	Details	
Cert	tificate <u>H</u> ierarchy	
~ K	KIBSTrust Root CA G2	
	✓ KIBSTrust Issuing Qsig CA G2	
	Imetest Prezime zemjodelec	
Cert	tificate <u>F</u> ields	
~ 1	metest Prezime zemjodelec	^
	✓ Certificate	
	Version	
	-Serial Number	
	Certificate Signature Algorithm	
	Issuer	
	✓ Validity	
Field	d Valua	*
FICK		
E	хроп	
		<u>C</u> lose

Слика 12

3. Како да направам безбедносна копија од сертификатот?

Вашиот сертификат е инсталиран на дискот на Вашиот компјутер и истиот може да биде избришан при појава на грешки во оперативниот систем или откажување на хардверот на Вашиот компјутер. За да го заштитите Вашиот сертификат во вакви ситуации, потребно е да направите безбедносна копија од сертификатот односно да го експортирате во .p12 датотека.

За да направите безбедносна копија од Вашиот сертификат треба да ги извршите следните чекори:

1. Од менито на прелистувачот во горен десен агол селектирајте **Options** (Слика 13):



Слика 13

2. Во новиот прозорец (Слика 14) од менито на левата страна изберете ја опцијата **Privacy & Security,** отидете најдолу, притиснете на копчето **View Certificate**<u>s</u>:

G Google	×	🔅 Options	×	+					_		×
← → ♂ ŵ	😫 Firefox	about:preference	s#privacy		80%	☆	Q Search			lii\	≡
					₽ Fin	d in Op	otions				^
General	Allow	Firefox to send <u>c</u> rash	reports to Mozilla	Learn more							
Privacy & Security	Q search Security Privacy & Security Security C Firefox Account Deceptive Content and Dangerous Software Protection ✓ Block dangerous and deceptive content Learn more ✓ Block dangerous downloads ✓ Warn you about unwanted and uncommon software										
⑦ Firefox Support	Certifica When a se Selec Ask y Certifi	tes erver requests your per t one automatically ou every time / OCSP responder serv cates	rsonal certificate rers to confirm the	current validity	of		View <u>C</u> ertificates Security <u>D</u> evices]			~

Слика 14

3. Од картичката Your Certificates (Слика 15) изберете го Вашиот сертификат и кликнете на копчето <u>Backup...</u>:

/ou have certificates fro	m these organizations that	t identify you:		
Certificate Name	Security Device	Serial Number	Expires On	Ę
Ime10 Prezime10	Software Security Dev	13:8F:0A:74:7C:51:65:.	26.11.2018	

Слика 15

 Изберете локација каде што ќе се зачува датотеката и внесете име на датотеката (Слика 16). Кликнете Save за да продолжите:

	==	-
		- *
Date modified	Туре	Size
15.12.2015 10:46	File folder	
11.1.2016 12:20	File folder	
11.1.2016 10:10	File folder	
	Date modified 15.12.2015 10:46 11.1.2016 12:20 11.1.2016 10:10	Date modified Type 15.12.2015 10:46 File folder 11.1.2016 12:20 File folder 11.1.2016 10:10 File folder



5. Внесете лозинка со која ќе го заштитите приватниот клуч (Слика 17). Поставената лозинка ја знаете само Вие, Ве молиме да ја запаметите или да ја запишете на безбедно место! Кликнете ОК за да продолжите:

Choose a Certificate Backup Password	Х
The certificate backup password you set here protects the backup file that you are about to create. You must set this password to proceed with the backup.	I
Certificate backup password:	
Certificate backup password (again):	
Important: If you forget your certificate backup password, you will not be able to restore this backup later. Please record it in a safe location. Password quality meter	
OK	

Слика 17

6. Ќе добиете порака дека успешно го експортиравте Вашиот сертификат (Слика 18):



ВАЖНО: .P12 датотеката во која е експортиран Вашиот сертификат и лозинката за истата зачувајте ги на безбеден надворешен медиум (надворешен хард диск, USB flash меморија, CD/DVD...)!

4. Како да го импортирам сертификатот во Internet Explorer?

За да импортирате сертификат во Internet Explorer (IE), прво треба да имате датотека од вашиот сертификат со екстензија .pfx или .p12, а потоа да ги извршите следните чекори: Bo Internet Explorer бирате Tools/Internet Options/Content/Certificates (или пак директно од **Manage User Certificates** конзолата) изберете **Certificates** (Слика 19), а потоа **Import** (Слика 20), Next (Слика 21), Browse (Слика 22).



Слика 19

Other Peop	le Intermediate Certificat	ion Authorities	Trusted Root Certification
Issued To	Issued By	Expiratio.	Friendly Name
Import Exp	port Remove		Adva
Import Exp ertificate intended p	port Remove		Adva

Слика 20

1		
	Welcome to the Certificate Import Wizard	
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	To continue, click Next.	
	Net	
	Слика 21	<
~	F Certificate Import Wizard	
	File to Import Specify the file you want to import.	
	File to Import Specify the file you want to import. File name: Browse	
	File to Import SpedFy the file you want to import. File name: I Browse Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange- PKCS #12 (.PFX,.P12)	
	File to Import Specify the file you want to import. File name: I Browse Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P78) Microsoft Serialized Certificate Store (.SST)	
	File to Import Specify the file you want to import. File name: I Browse Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange- PKCS #12 (.PFX, P.12) Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P78) Microsoft Serialized Certificate Store (.SST)	
	File to Import Specify the file you want to import. File name: Import Decomposition Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P78) Microsoft Serialized Certificate Store (.SST)	

Слика 22

Потоа потврдете го направениот избор со кликање на **Next** (Слика 23).

ile to Ir	nport
Spe	cify the file you want to import.
File	name:
C:	\Users\ileg\Desktop\ImeAdvTretPrezimeAdvTret.p12 Browse
Not	e: More than one certificate can be stored in a single file in the following formats:
F	Personal Information Exchange- PKCS #12 (.PFX,.P12)
(Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
I	Microsoft Serialized Certificate Store (.SST)



Ставете ја лозинката од бекап фајлот изберете ја опцијата "Mark the private key as exportable" и изберете Next (Слика 24).

riva	ate key protection
	To maintain security, the private key was protected with a password.
	Type the password for the private key.
	Password:
	•••••
	Display Password
	Import options:
	Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
	Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
	Protect private key using virtualized-based security(Non-exportable)
	☑ Include all extended properties.

Слика 24

Изберете Изберете ја опцијата "Automatically select the certificate store based on the type of certificate", потоа избирајте **Next** како на Слика 25 и на крај **Finish**.

	te stores are svs	tem areas where	certificates are	kept.	
Window the cert	s can automatical ificate.	lly select a certifi	cate store, or yo	u can speci	fy a location for
۹	utomatically selec	t the certificate	store based on t	he type of (certificate
OP	ace all certificates	s in the following	store		
C	ertificate store;				
	Personal				Browse

Слика 25

Сертификатот сега треба да се појави во Вашата листа на лични сертификати (Слика 26):

Certificates					×
Intended purp	pose: <	All>			~
Personal (Other People	Intermediate Certific	cation Authorities	Trusted Root Cert	ification 1 🕨
Issued To) dvTret Prezim	Issued By KIBSTrust Issuing	Expiratio 9 Qsi 26.5.20	o Friendly Nam 22 ImeAdvTret I	e Prez
Import	Export	t <u>R</u> emove		[Advanced
– Certificate i	ntended purp	oses			View
					<u>C</u> lose



Вака импортиран сертификатот е достапен и преку прелистувачот Google Chrome.

5. Проверка на коренски сертификати во Internet Explorer

Со двоен клик на сертификатот (Слика 26) отворете го и проверете дали во табот Certification Path приказот е како на Слика 27, односно дали се прикажува ланец од вашиот сертификат и:

- коренски сертификат KIBSTrust Root CA G2 и
- издавачки KIBSTrust Issuing Qsig CA G2 или KIBSTrust Issuing Qseal CA G2

💼 Certificate	×
General Details Certification Path	
Certification path	AD Skopje ID
	View Certificate
Certificate status: This certificate is OK.	
	OK

Слика 27

Доколку во приказот над вашиот сертификат недостасува некој од коренските сертификати на издавачот KIBSTrust, Ве молиме да ги преземете од секцијата **Коренски сертификати** од <u>https://www.kibstrust.com/mk-MK/Home/Support/</u> и да ги инсталирате:

KIBSTrust Root CA G2 (Инсталирајте ги во Trusted Root Certficate Authorities)

KIBSTrust Issuing Qsig CA G2 (Инсталирајте ги во Intermediate Certificate Authorities)

KIBSTrust Issuing Qseal CA G2 (Инсталирајте ги во Intermediate Certificate Authorities)

* * *